SECURING AI ADOPTING

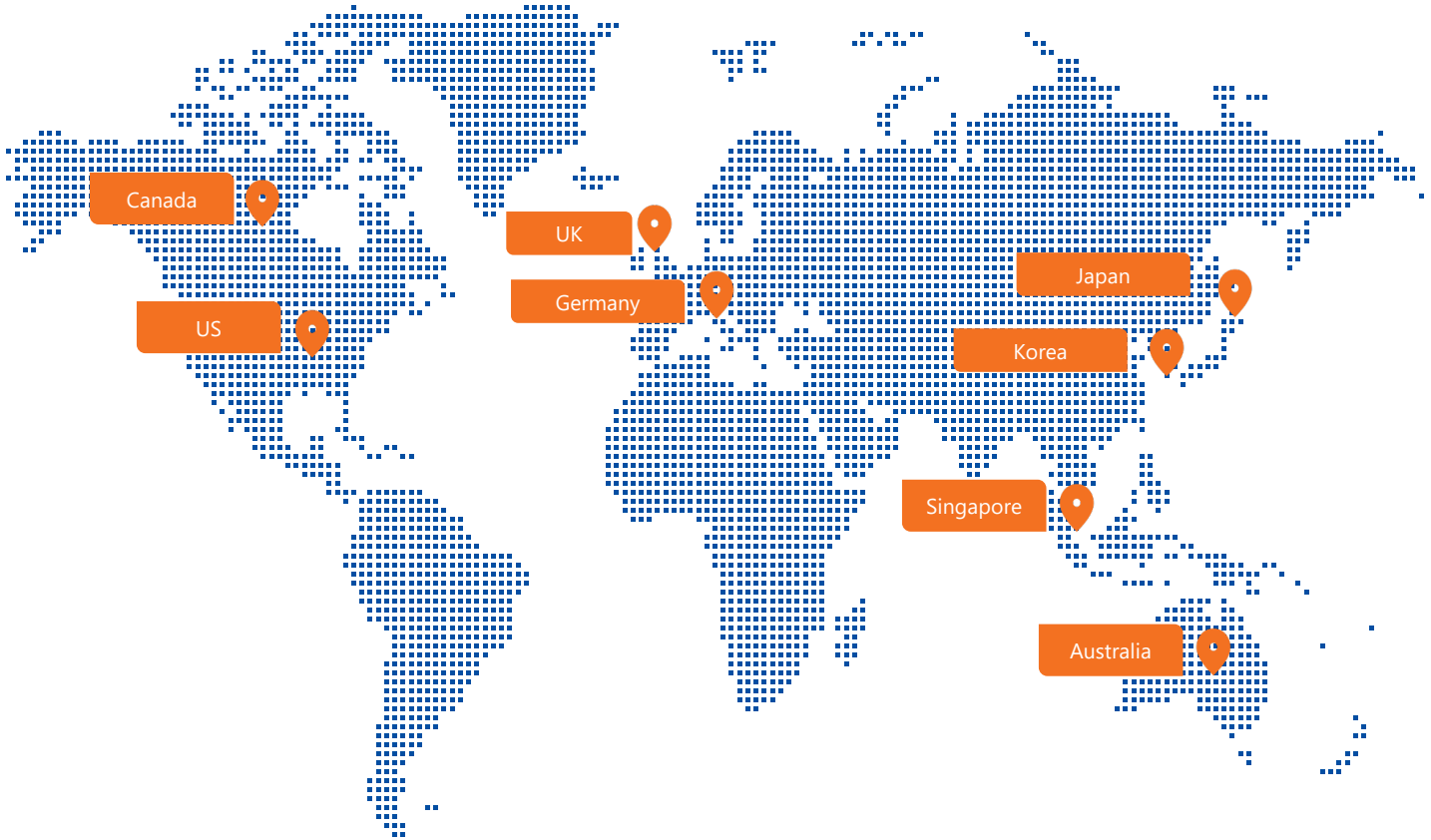
A TRUSTED PARTNER IN DIGITAL TRANSFORMATION

Discovering threats earlier and responding in a way that minimizes damage for your organization

300+
Engagements/Year

6
Industries

99+
Customer Satisfaction Score



SECURITY CERTIFICATIONS

CREST | PEN TEST | SOC | ISO 27001 Certified | ISO 20000 Certified

SELECTED PERSONNEL CERTIFICATIONS

CISSP – Certified Information Systems Security Professional
CCSP – Certified Cloud Security Professional
CSSLP – Certified Secure Software Lifecycle Professional

OSWE | OSCE | OSCP | GWAPT | CEH Certified Ethical Hacker

AWS Certified Solutions Architect Professional | AWS Certified Security Specialty | Microsoft Certified Cybersecurity Architect Expert | CompTIA CySA+ | ECIH EC-Council Certified Incident Handler

AN END-2-END CYBERSECURITY SERVICE PROVIDER

Our services cover full spectrum, from Defensive to Offensive Technology, focusing on Cloud and Application Security

VERTICAL

- Healthcare
- Banking & Finance
- Manufacturing

EXPERTISE & SERVICE

Offensive Security

- Penetration Testing as a Service
- Red Team Service
- Cloud Security Assessment

Digital Risk Management

- Security Controls Review
- Application Security & DevSecOps
- Cybersecurity Maturity Assessment

Cyber Defense

- SOC as a Service
- Managed Extended Detection & Response
- Use Case Engineering

Cloud & AI Security

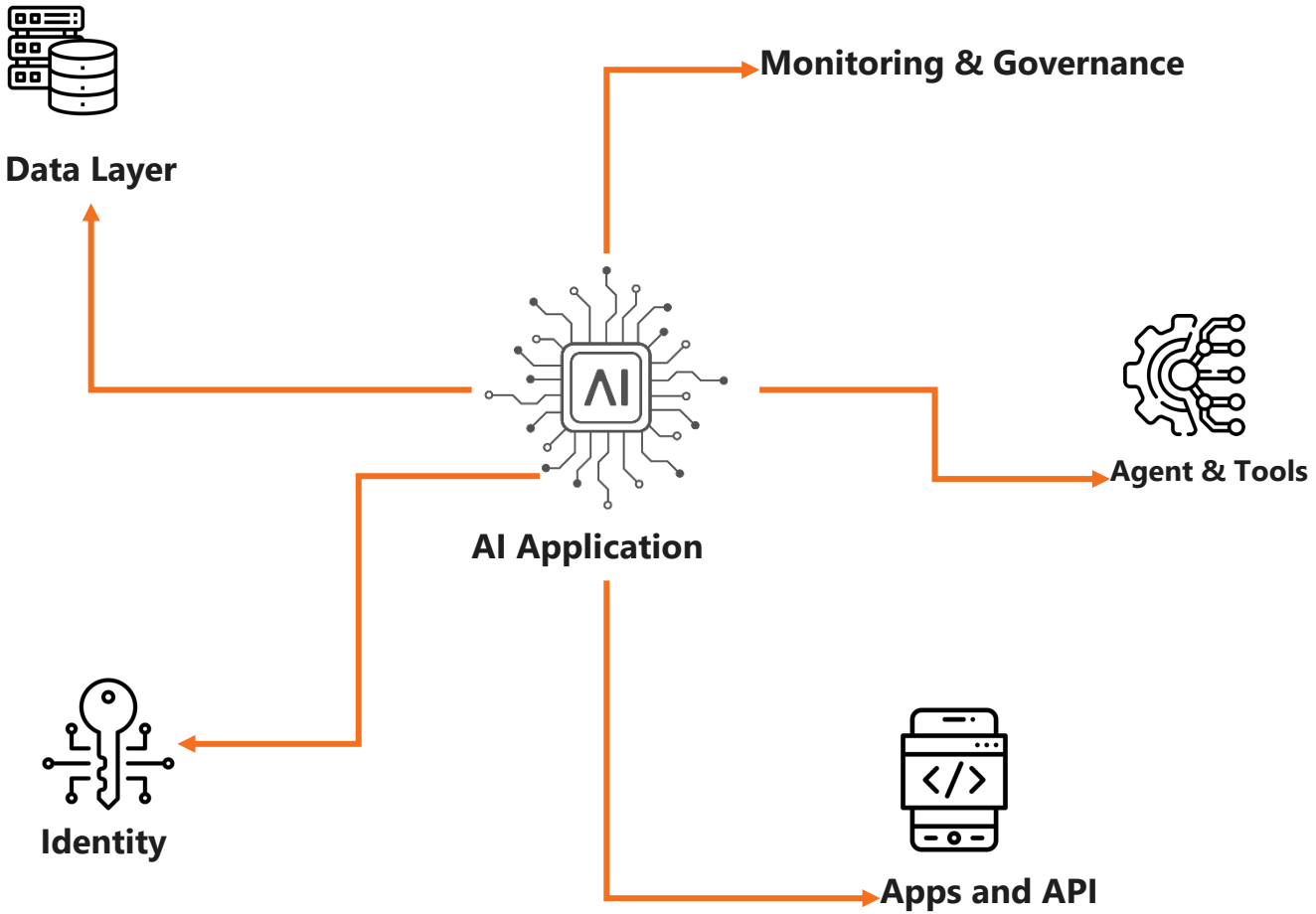
- AI Security Consulting
- Cloud and Data Security
- Microsoft Security

ENABLERS

- Best shore Delivery Model
- Software Defined Security
- Scale Fast
- Solution Library
- Factory Delivery (Use Case, Pentest)
- Product First

Securing AI Adoption: Enable Innovation Without Increasing Risk

Agentic AI and enterprise data layers create new paths for data leakage and unauthorized actions. Security must be end to end.



Outcomes

- Protect sensitive data across prompts, grounding, and connectors
- Control agent identities and permissions with Zero Trust principles
- Maintain compliance and auditability while scaling AI faster

AI security is not only model security. It is data, identity, app, agent, and operations security.

Key Security Risks in Agentic AI and Data

As AI connects to enterprise data and tools, the attack surface expands beyond traditional apps

USD 4.44M

Global average breach cost fell 9 percent to **USD 4.44 million**. US costs rose 9 percent to a record USD 10.22 million, driven by higher fines and detection and escalation costs. [1]

97%

Share of organizations that reported an AI-related breach and lacked proper AI access controls. Most incidents came via the AI supply chain through compromised apps, APIs, or plug ins, often causing broad data compromise and operational disruption, showing ***AI is becoming a high value target.*** [2]

63%

Share of organizations that lack AI governance policies are still creating one, and many also lack approval processes, governance technology, and audits for unsanctioned AI. Overall, ***AI adoption is outpacing security and governance, leaving usage largely unchecked.*** [3]

[1][2][3] IBM Cost of a Data Breach Report 2025

Agent & Application Risks

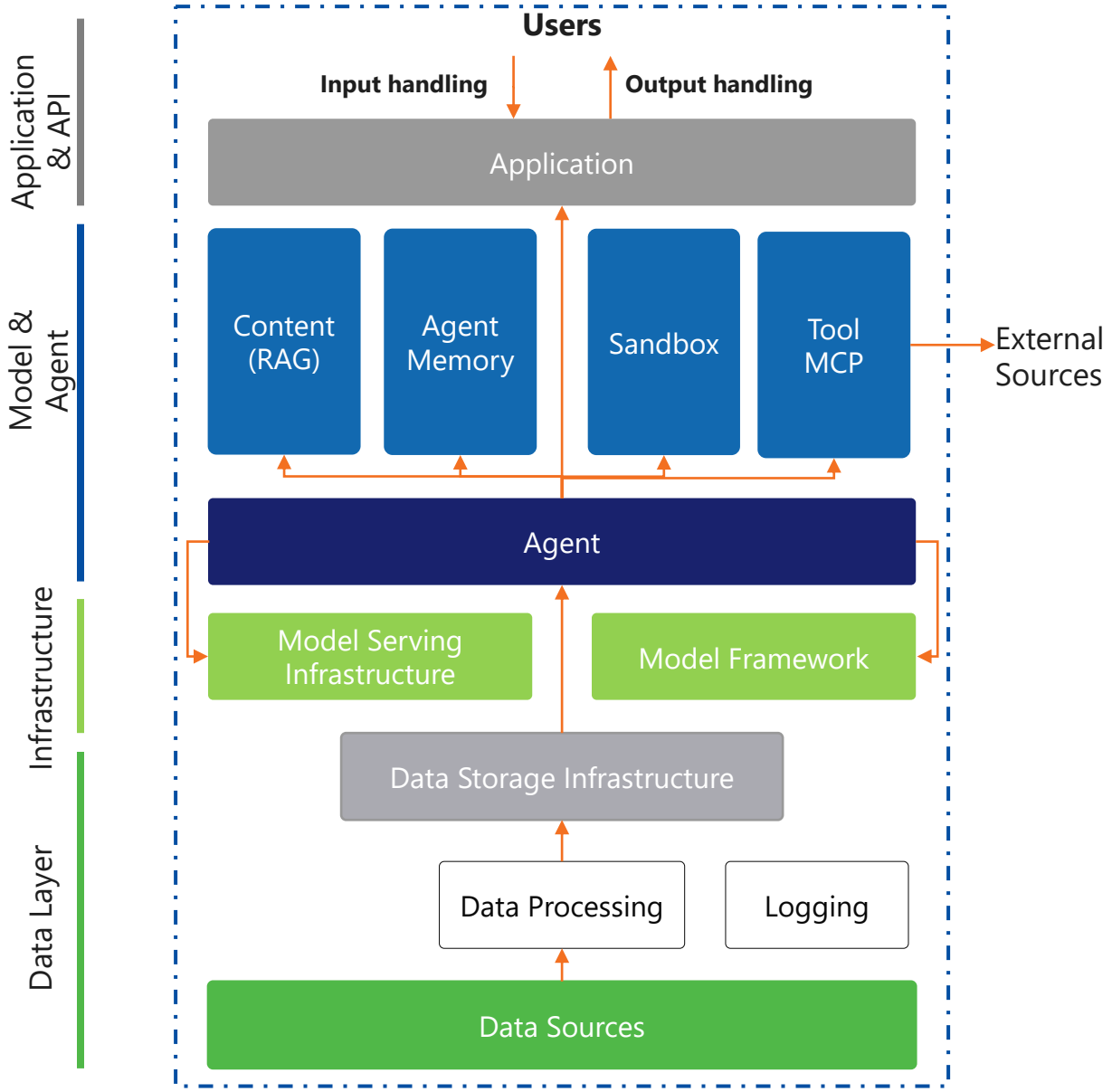
- Prompt injection leading to unsafe tool calls or data exfiltration
- Over permissioned agents and connectors acting beyond intent
- Insecure APIs and plugins enabling lateral movement
- Lack of monitoring: limited traceability of actions and decisions

Data Risks

- Sensitive data leakage from grounding sources and chat history
- Data poisoning and integrity issues in curated knowledge bases
- Over sharing via vector stores and search indexes
- Weak data governance: unclear lineage, labeling, retention

Secure by Design Architecture for AI Applications

Standard controls extended to AI data flows, agents, and model interactions



Application and API security:

- Authenticate, authorize per action, and restrict scopes to least privilege
- Validate inputs, enforce schemas, and apply rate limiting to reduce abuse and injection paths

Model and prompt guardrails:

- Prompt injection defenses, content filtering, safe tool use policies
- Input/Output controls and policy-based grounding, PII

Agent Identity & Access:

- Least privilege for agents/multi-agents and workloads
- Access management

Securing Infrastructure:

- Isolate inference services
- Runtime hardening and isolation
- Secure secrets and keys

Data protection and governance:

- Classify and label data, DLP, encryption, retention
- Control grounding sources and vector stores

Monitoring:

- Logging and tracing of agent actions
- Monitoring for malicious user behavior

FPT's Secure AI Adoption Roadmap

From assessment to secure rollout for agentic AI, RAG, and enterprise data integration.

Discover and Assessment

- Inventory AI use cases, agents, connectors, data sources
- **Map end to end data flows** (prompts, grounding, vector stores, tool calls)
- Identity, data protection, DLP, and secure integration patterns
- **Threat model and risk assessment** for top scenarios (leakage, tool misuse, over permission)

Design and build guardrails

- Secure app and API layer: allow list, input validation, logging standards
- **AI Secure Coding Skillset** that enforces security best practices in every AI generated code output
- **Secure reference architecture for AI apps and model serving**:
  - Prompt Shield
  - PII / Secret Masking
  - Sandbox Isolation
  - MCP Security Connector
  - RBAC

Validate and hardening

- Validate connector permissions for agents and workflows
- **Security testing of APIs and infrastructure** (config review, vulnerability scanning, hardening)
- **AI Penetration Testing**:
  - Sandbox Evasion
  - Memory Poisoning
  - Guardrail bypass
  - Jailbreak

Steady State

- **Regular AI Penetration Testing** (Quarterly)
- Governance: access reviews, policy updates, prompt maintain
- **AI Risk Assessment** followed by standards:
  - NIST AI RMF
  - SOC 2
  - EU AI Act
  - GDPR
  - ISO/IEC 42001:2023

We adhere to industry-leading standards and best practices

- OWASP Top 10 for Large Language Model Applications
- OWASP AI Security and Privacy Guide
- Google's Secure AI Framework (SAIF)
- Adversarial Threat Landscape for Artificial-Intelligence Systems
- NIST AI Framework

DATA SECURITY AND GOVERNANCE FOR AI

Helping organizations protect personal data, meet global regulatory requirements.

FPT leverages Microsoft Purview to secure the data that powers AI and Copilot, helping organizations prevent sensitive data exposure, enforce access and usage controls, and meet global regulatory requirements.

Our approach combines data classification and labeling, DLP and insider risk controls, compliance automation, and continuous monitoring across Microsoft 365 and multi cloud data sources to enable safe, governed AI adoption at scale.

Prevent sensitive data leakage

Compliance and audit readiness

Safe AI adoption at scale

OUR OFFERING – Powered by Microsoft Purview

Discovery

- Assess current data security and compliance posture using **Microsoft Compliance Manager**
- Establish a **regulatory baseline** mapped to applicable requirements (e.g. PDPA, GDPR, AI-related obligations)
- Identify high-risk data types and locations using **Data Risk Assessment**
- Map Copilot/AI data access paths across Microsoft 365 workloads

Protect

- Design and implement data classification and labelling strategies aligned with regulatory needs
- Configure DLP policies to reduce Copilot/AI driven oversharing and data misuse
- Apply protection controls consistently across cloud and hybrid environments

Govern

- Map Copilot/AI governance controls to:
  - **NIST Cybersecurity Framework** (Identify, Protect, Detect, Respond, Recover)
  - **Zero Trust principles**, including identity, data, and least-privilege access
- Establish AI-aware governance policies for data access, retention, and usage
- Strengthen auditability and explainability of Copilot-assisted/AI data access

AI SECURITY CONSULTING

As enterprises increasingly integrate AI into their operations, new security challenges emerge that traditional measures often fail to address. AI-driven systems can introduce unique vulnerabilities, requiring specialized testing to safeguard against exploitation. Our AI consulting services focus on pinpointing and resolving the specific security gaps your business faces, ensuring your AI applications remain secure, reliable, and resilient.

1. **Insecure AI deployment**
2. **AI Application**
3. **Trust and Safety**

OUR OFFERING

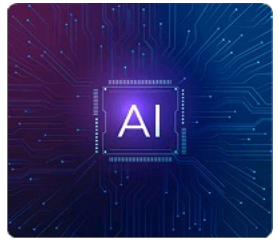
AI Security Penetration Testing

AI Penetration Testing is our specialized service for testing and securing both generative and non-generative models or applications integrated with AI features, identifying threats, addressing vulnerabilities, and ensuring safety and reliability before rollout using globally recognized security standards.

AI Risk Assessment

FPT conducts risk assessments for AI applications, addressing traditional threats and AI-specific vulnerabilities like prompt injections and data exfiltration. It ensures compliance with industry standards and FPT Software certifications for secure and trustworthy deployment.

CHALLENGE WITH AI ADOPTION IN BUSINESS

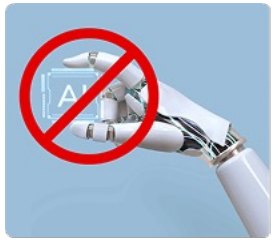


98%

Of companies consider certain AI models critical to business success, driving efficiency, innovation, and competitive advantage.

77%

Organizations have experienced AI system breaches that exposed sensitive data, disrupted operations, and undermined trust in AI driven processes.



54%

Of consumers do not trust AI due to data security and privacy concerns, highlighting data handling as a key barrier to adoption.

AI SECURITY PENETRATION TESTING

AI Security Penetration Testing ensures AI models or applications are tested, secured, and ready for safe rollout by addressing vulnerabilities using trusted global security standards.

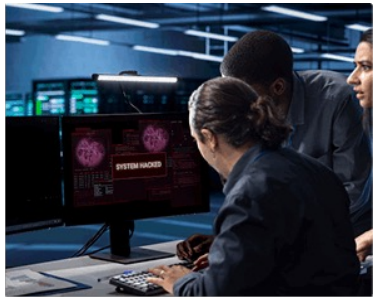
What We Do

- **Assess system capabilities and context** by understanding the system's purpose and the risks it introduces
- **Uncovers** unknown vulnerability and benchmarking assesses known vulnerabilities.
- **Automate** use automation to scale attack coverage.
- **Measure** design structured scenarios to assess AI behavior that violates ethical principles even when security controls pass.
- **Recommendation** on how to mitigate vulnerabilities on production environment

Benefits

Best practice assurance

AI's complexity demands proactive security, as traditional measures may fall short against advanced threats.



Regulatory compliance

Align industry standards with your environment, tailored to meet your specific needs

Data security

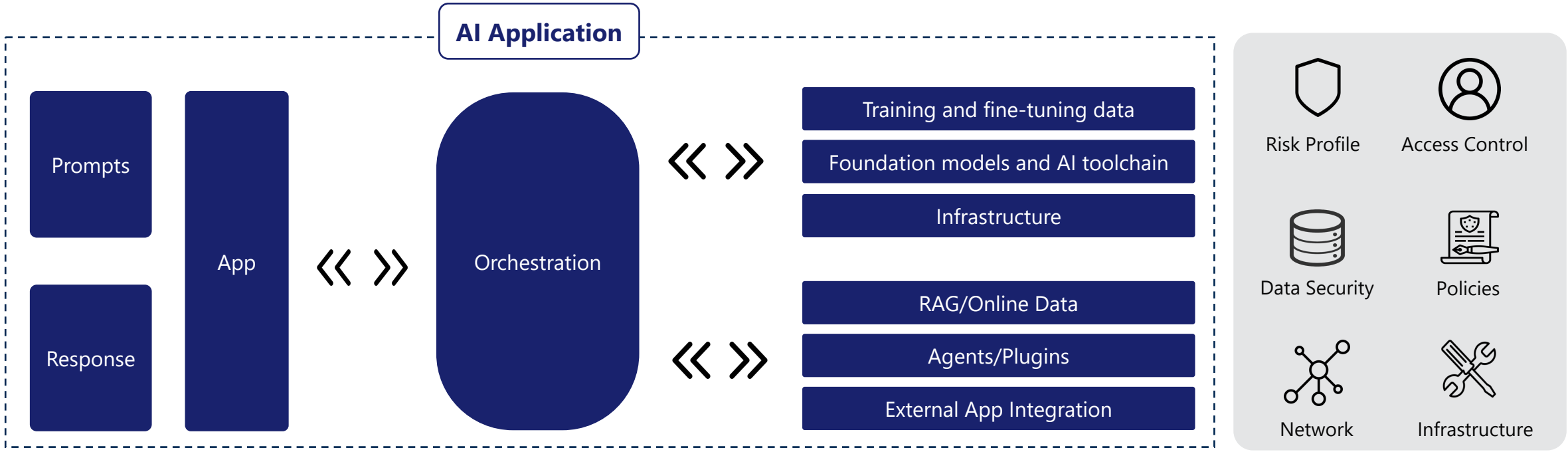
AI systems process sensitive user data like names, contacts, and payments. Security testing identifies vulnerabilities to protect this data from exploitation.

We adhere to industry-leading standards and best practices

- OWASP Top 10 for Large Language Model Applications
- OWASP AI Security and Privacy Guide
- Google's Secure AI Framework (SAIF)
- Adversarial Threat Landscape for Artificial-Intelligence Systems

AI RISK ASSESMENT

The Risk Assessment helps businesses assess AI risks, ensure compliance, and align solutions with FPT Software certifications for secure and reliable deployment.



Our Solution

- **Security review** your AI Application from Development to Deployment
- Correlation between Penetration Testing Report and Compliance Report
- Deliver real-time **compliance status** and review insights on a dashboard with supporting evidence documentation

Key Benefits

- **Reviewed and Certified** by FPT Software
- **Simplified Compliance Sharing** streamlines the process of sharing security and compliance documentation, making it easier to provide customers and stakeholders with up-to-date reports, certifications, and audits
- **Enhanced Transparency and Trust** with clients, demonstrating a commitment to security and regulatory compliance

Success Stories

Secure by Design AI Agent SaaS Platform (NIST AI RMF Aligned)

Brief

A customer set out to build an AI agent platform and commercialize it as a SaaS offering for external clients. FPT engaged from version one to **define the secure architecture, build the security baseline, and embed security into the product delivery lifecycle**. We also supported their engineering team as they used AI assisted coding during development.

Challenge

As a multi tenant SaaS with agent capabilities, the product had to prevent tenant data leakage, over permissioned agents, and misuse of integrations, jailbreak while staying compliant and scalable. **Rapid feature delivery** increased the risk of security and inconsistent controls across new capabilities. **AI generated code introduced additional risk of insecure patterns and vulnerable dependencies entering the codebase.**

Results

Security became a product feature from day one, with controls implemented and continuously validated against **NIST AI RMF** as the platform evolved. Ongoing security testing at each release reduced production risk, shortened approval cycles, and improved buyer trust for enterprise customers. **The team also adopted an internal secure coding AI skill that guided code generation toward secure patterns and reduced recurring vulnerabilities.**

AI Penetration Testing Uncovered Critical Agent Exploitation Risk

Brief

FPT performed an AI Penetration Testing of an Enterprise Chat Assistant built on a multi agent architecture with tool integrations and access to internal data sources. The scope covered prompt and agent interactions, tool call flows, data access, and the Azure hosting and identity dependencies. Our objective was to **validate whether existing guardrails were sufficient for a production rollout.**

Challenge

The application **already implemented multiple prevention layers, including guardrails, content controls, and sandboxing intended to limit unsafe actions**. However, multi agent orchestration and trusted tool chains increased complexity and introduced indirect paths that could be abused.

Results

We **demonstrated a critical business risk where the assistant could be manipulated to access sensitive enterprise data and trigger high impact actions** in the connected Azure environment. This provided clear evidence to **reprioritize security controls before production rollout**. The outcome was a remediation roadmap that reduced exposure, strengthened governance, and increased confidence for safe scale up.

THANK YOU